Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC. 20554

In the Matter of:	)	
	)	
Communications Assistance for	)	CC Docket No. 97-213
Law Enforcement Act	)	

COMMENTS OF U S WEST, INC.

Of Counsel

Dan L. Poole
U S WEST, Inc.

William T. Lake
John H. Harwood II
Lynn R. Charytan
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420
(202) 663-6000

Kathryn Marie Krause
Edward M. Chavez
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Counsel for

U S WEST, INC.

December 14, 1998

SUMMARY

The FNPRM correctly separates the analysis of CALEA capabilities into two parts: first, whether a capability falls within the scope of section 103(a) and, second, whether such a capability can be justified in light of the cost, privacy, and other considerations enumerated in section 107(b). Applying the first prong of the test, the FNPRM appropriately excludes three of the "punch list" capabilities demanded by DOJ/FBI, but erroneously includes five of the capabilities as well as the location information capability contained in J-STD-025. None of these capabilities should be included in a Commission standard, either because law enforcement may not use them consistently with Title III or the ECPA, or because they would expand the capabilities available to law enforcement rather than maintain the status quo as Congress intended.

In any event, DOJ/FBI has failed to carry its burden under the second prong of the test: to show that each capability passes muster under section 107(b). Under Commission precedent and basic evidentiary principles, DOJ/FBI must come forward with the comprehensive cost data regarding the punch list that only it possesses or face the presumption that the data does not support its case. As the petitioner in this proceeding, DOJ/FBI also bears the burden of showing, under section 107(b), that each capability would be cost-effective and would not unduly raise residential rates.

The Commission should in no event obligate carriers to separate the "headers" from content in order to provide law enforcement call-identifying information on packet-switched networks. Such a requirement is not technologically feasible. Indeed, the risks to advanced services and the Internet strongly suggest that the imposition of *any* CALEA

requirements on packet networks should be deferred, at least until CALEA can be implemented without inhibiting the development of advanced telecommunications services.

U S WEST supports the FNPRM's tentative conclusion that the Commission should remand any necessary technical standardization work to TIA's Subcommittee TR45.2. However, the Commission's expectation that Subcommittee TR45.2 will be able to complete this process within 180 days after the Commission releases an order in this proceeding probably is overly optimistic. Subcommittee TR45.2 has been working on CALEA's technical requirements for some time but, depending on how many of the punch list capabilities that the Commission ultimately adopts and on how the Commission defines those capabilities, developing a consensus on the necessary technical standards and having them subsequently approved by ballot (as required under American National Standards Institute ("ANSI") procedures) could take more than one year.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC. 20554

In the Matter of:	)	
	)	
Communications Assistance for Law Enforcement Act	)	CC Docket No. 97-213
	)	

COMMENTS OF U S WEST, INC.

U S WEST, Inc.[1] ("U S WEST") submits these comments on the Further Notice of Proposed Rulemaking ("FNPRM") issued in response to the deficiency petitions filed by the Department of Justice and the Federal Bureau of Investigation ("DOJ/FBI") and the Center for Democracy and Technology ("CDT").[2] The FNPRM correctly proposes to analyze whether each capability requirement demanded by DOJ/FBI or challenged by CDT, first, falls within the scope of section 103(a) of CALEA and, second, if it does, can be required consistently with the cost and privacy considerations of section 107(b). Applying the first prong of the test, the FNPRM appropriately excludes three of the "punch list" capabilities demanded by DOJ/FBI, but erroneously includes five of the capabilities as well as the location information capability contained in J-STD-025. As set forth below, *none* of the punch list capabilities meets the requirements of section 103(a). In any event, DOJ/FBI has failed to carry its burden under the second prong of the test: to show that each capability passes muster under section 107(b).

1/ U S WEST provides communications services to over 25 million customers nationally and in 14 western and mid-western states. The company's primary products and services include: local telephone services; long distance; wireless PCS service in selected markets; custom calling service; local phone interconnections to interstate long-distance companies; operator services; and a host of high-speed data networking services and equipment.

2/ *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Further Notice of Proposed Rulemaking, FCC 98-282 (rel. Nov. 5, 1998).

DOJ/FBI has that burden because it is the petitioning party here and because only DOJ/FBI has access to the apparently comprehensive estimates that manufacturers prepared earlier this year concerning the costs of developing CALEA-compliant products. It also would be premature for the Commission to impose any compliance obligations with respect to rapidly developing packet-mode technologies and the advanced services using them, and the Commission should in no event require carriers to take the technologically infeasible step of separating header information from call content. Finally, if the Commission decides to include any of the disputed capabilities in a standard, it should (as the FNPRM tentatively concludes) remand any necessary technical tasks to Subcommittee TR45.2 of the Telecommunications Industry Association ("TIA").

I. CALEA REQUIRES SEPARATE INQUIRIES UNDER SECTIONS 103(a) AND 107(b), AND DOJ/FBI BEARS THE BURDEN OF SHOWING THAT EACH CAPABILITY MEETS THE REQUIREMENTS OF SECTION 107(b).

As required by the Act, the FNPRM separates the analysis of CALEA capabilities into two parts: first, whether a capability falls within the scope of section 103(a), and, second, whether the inclusion of such a capability can be justified in light of the cost, technical, and privacy considerations enumerated in section 107(b).[3/] As U S WEST earlier demonstrated in its comments on the Public Notice, CALEA establishes a limited *quid pro quo*: Law enforcement obtains certain limited electronic surveillance capabilities, and both carriers and the ratepaying public are protected against unreasonable costs.[4/] One of CALEA's chief protections against

---

3/ *See* FNPRM at ¶ 29.

4/ *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Comments of U S WEST, Inc., at 1 (filed May 20, 1998) ("*U S WEST Public Notice*

(continued...)

such costs is section 107(b), which proscribes the imposition of capability requirements if costs are excessive.[5/]

Thus, the Commission appropriately seeks specific information regarding whether each of the disputed punch list capabilities meets the various factors of section 107(b).[6/] To apply section 107(b), the Commission needs to know what manufacturers will charge carriers for CALEA-compliant products and what costs carriers will incur in installing those products. Without such information, the Commission cannot make a reasoned decision about whether a capability can be implemented "by cost-effective methods" or in such a way as to "minimize the cost . . . on residential ratepayers." *See* 47 U.S.C. § 1006(b)(1), (3). In the words of Commissioner Furchtgott-Roth, "the Commission must understand the balance of costs and benefits . . . of the choices before [it]."[7/]

Under principles long applied by the Commission and the courts, DOJ/FBI is obligated here both to come forward with whatever information it has about the costs or expected prices of manufacturers for CALEA solutions and to demonstrate, based on that information, that the requirements of section 107(b) are satisfied for each disputed capability requirement that falls within the scope of section 103(a): that the capability can be implemented "by cost-effective methods" and in such a way as to "minimize the cost . . . on residential ratepayers." *See* 47

4/ (...continued)
Comments").

5/ *Id.* at 9.

6/ *See* FNPRM at ¶ 30; *see also* FNPRM, Separate Statement of Commissioner Harold W. Furchtgott-Roth.

7/ FNPRM, Separate Statement of Commissioner Harold W. Furchtgott-Roth.

U.S.C. § 1006(b)(1), (3). As discussed more fully below, some manufacturers recently have provided some carriers, including U S WEST, with estimates of the manufacturers' prices for supplying comprehensive CALEA solutions for the carriers' entire networks. However, the manufacturers have not provided U S WEST with a breakdown of the costs of individual punch list items or other capabilities. In contrast, U S WEST understands that manufacturers have provided just such information to DOJ/FBI: the manufacturers' estimates of their costs for developing products that comply with J-STD-025 and each of the punch list items.

In these circumstances, DOJ/FBI plainly must come forward with that information, explain the methodologies under which the costs were calculated, and demonstrate that requiring carriers to implement individual punch list items would be cost-effective and would not unduly burden residential ratepayers.[8/] A party with unique access to relevant evidence must either present the evidence or face the presumption that the evidence is harmful to that party.[9/] In Commission proceedings, for example, the burden of production is routinely placed on parties that have peculiar knowledge of operative facts.[10/] Indeed, the "adverse

---

8/ USTA and other industry associations recently sent a letter to Attorney General Reno, officially requesting that DOJ/FBI submit all of its cost data to the Commission. *See* Letter to Attorney General Janet Reno from Roy Neel, Jay Kitchen, Matthew Flanagan, and Thomas Wheeler, December 4, 1998. U S WEST fully supports this request.

9/ *See* 2 Wigmore, *Evidence* § 285 (Chadbourn rev. 1979) ("The failure to bring before the tribunal some circumstance, document, or witness, when either the party himself or his opponent claims that the facts would thereby be elucidated, serves to indicate, as the most natural inference, that the party fears to do so; and this fear is some evidence that the circumstance or document or witness, if brought, would have exposed facts unfavorable to the party.").

10/ *See Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket No. 96-149, First Report and Order and Further Notice of Proposed Rulemaking, 11 FCC Rcd 21905, 22072 ¶ 345 (1996) ("*Non-Accounting Safeguards Order*") (placing burden of production on "the party most likely to have (continued...)

inference rule" is applied as a matter of course in both civil litigation and administrative proceedings.[11/] Under that rule, "the omission by a party to produce relevant and important evidence of which he has knowledge, and which is peculiarly within his control, raises the presumption that if produced the evidence would be unfavorable to his cause."[12/] Without this rule, the search for truth by courts and agencies would be frustrated, and opposing parties without access to evidence would be unfairly disadvantaged. If DOJ/FBI does not provide all of its cost information (including a full explication of the assumptions and bases for its ultimate cost figures), the Commission must presume that the punch list capabilities do not meet the criteria of section 107(b). Any other result would unfairly prejudice carriers and ratepayers, who would be forced to bear costs that never have been shown to be reasonable.

Carriers also must be afforded an adequate opportunity to review DOJ/FBI's cost data and present their views on the data's significance to the Commission. Both the Commission and the courts have recognized that interested parties must be given an opportunity to challenge and give their different perspectives on materials on which the agency relies when making a

---

10/ (...continued)
relevant information in its possession"); *Application of Illinois Bell Telephone Co.*, CC Docket No. 78-314, Memorandum Opinion and Order, 69 F.C.C.2d 1199, 1213 ¶ 32 (1978) (placing burden of production and burden of proof on party that had "sole possession" of key information); *United Telephone Co. of Ohio*, Docket No. 19072, Memorandum Opinion and Order, 26 F.C.C.2d 417, 421 ¶ 11 (1970) (stating that "burden of going forward with the introduction of evidence and the burden of proof should be on the petitioning party").

11/ *See Vodusek v. Bayliner Marine Corp.*, 71 F.3d 148, 156-57 (4th Cir. 1995); *Evans v. Robbins*, 897 F.2d 966, 970 (8th Cir. 1990); *Callahan v. Schultz*, 783 F.2d 1543, 1545 (11th Cir. 1986); *International Union (UAW) v. NLRB*, 459 F.2d 1329, 1336-42 (D.C. Cir. 1972).

12/ *Tendler v. Jaffe*, 203 F.2d 14, 19 (D.C. Cir. 1953).

decision.[13] Such input from carriers will be crucial in this proceeding: The relevant cost data are no doubt based on assumptions and estimates that require external review and independent analysis. Any concerns about the confidentiality of the cost data can be addressed in the first instance by making it available in a form that aggregates the manufacturers' information, so long as the costs are broken out for each punch list item. Otherwise, a protective order may be appropriate.[14]

The burden also must be on DOJ/FBI to show that each capability would be cost-effective and would not unduly raise residential rates. DOJ/FBI is the petitioner in this proceeding and therefore must bear the burden of persuasion.[15] CALEA reinforces this

---

[13] *See, e.g., Examination of Current Policy Concerning the Treatment of Confidential Information Submitted to the Commission*, GC Docket No. 96-55, Report and Order, FCC 98-184, ¶ 44 & n.146 (rel. Aug. 4, 1998) ("*Confidential Information Order*"); *Abbott Laboratories v. Young*, 691 F. Supp. 462, 467 (D.D.C. 1988) (requiring disclosure to ensure that interested parties have meaningful opportunity to participate in rulemaking).

[14] *See Confidential Information Order* ¶ 45.

[15] *See, e.g.*, 47 C.F.R. § 1.773(a) (placing burden of proof on petitioner in proceedings seeking suspension of tariff filings); *Paragon Cable Torrance, El Segundo, Gardena, Hawthorne, and Lawndale, California*, CSR-4255-A, Memorandum Opinion and Order, 10 FCC Rcd 9462, 9466 ¶ 12 (1995) (finding that petitioner had not met its burden of proof when asking Commission to modify market boundaries under section 614(h)(1)(C) of the Communications Act); *Non-Accounting Safeguards Order*, 11 FCC Rcd. at 22072 ¶ 346 ("[I]n a typical complaint proceeding, the complainant has the burden of establishing that a common carrier has violated the Communications Act or a Commission rule or order."); *cf.* 5 U.S.C. § 556(d) ("[T]he proponent of a rule or order has the burden of proof."); 47 U.S.C. § 157(a) ("Any person or party . . . who opposes a new technology or service proposed to be permitted under this Act shall have the burden to demonstrate that such proposal is inconsistent with the public interest.").

conclusion by establishing that an industry standard is a presumptive safe harbor for carriers unless law enforcement or other parties can make an affirmative showing of deficiency.[16/]

What is more, DOJ/FBI's burden is a heavy one, given the evident magnitude of the costs of complying with J-STD-025 and the punch list items. DOJ/FBI itself has told Congress that, if the "grandfather" date in CALEA is moved from January 1, 1995 to the year 2000, that alone will increase the government's costs of securing compliance by more than $2 billion over and above the $500 million already authorized by the act.[17/] Thus, DOJ/FBI implicitly acknowledges that industrywide compliance with CALEA will cost more than $2.5 billion. Indeed, the cost undoubtedly will be more. Based on data collected from some of its members, the United States Telephone Association ("USTA") estimates that local exchange carriers alone would have to spend between $2.2 and $3.1 billion to implement J-STD-025 and six of the punch list capabilities.[18/]

16/ *See* 47 U.S.C. § 1006(a)(2) ("A telecommunications carrier shall be found to be in compliance with the assistance capability requirements . . . if the carrier . . . is in compliance with . . . standards adopted by an industry association or standard-setting organization . . . ."); *see also* H.R. Rep. No. 103-827, pt. 1, at 26 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3506 (noting that CALEA "establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations").

17/ *See* Letter from Attorney General Janet Reno to Senator Ted Stevens, October 6, 1998.

18/ *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Comments of the United States Telephone Association (filed Dec. 14, 1998). These numbers are, of course, only preliminary estimates. The exact cost will depend on a variety of factors, including the exact capabilities that carriers are required to provide, how quickly DOJ/FBI demands that carriers deploy the capabilities throughout their networks, and how manufacturers decide to implement the capabilities in their software upgrades.

II. THE COMMISSION STANDARD SHOULD NOT INCLUDE ANY OF THE PUNCH LIST CAPABILITIES OR THE LOCATION INFORMATION CAPABILITY.

None of the proposed punch list capabilities or the location information capability should be included in a Commission standard. As set forth below, U S WEST maintains its general support for J-STD-025. The Commission's proposed exclusion of three of the capabilities demanded by DOJ/FBI is sound; including the other disputed capabilities would be contrary to section 103(a), as demonstrated by both Title III and CALEA's legislative history.

A. The FNPRM Disregards the Relationship between CALEA and Title III, as Well as CALEA's Legislative History, When Evaluating Whether Capabilities Are Required under Section 103(a).

The FNPRM largely disregards Title III[19/] and the Electronic Communication Privacy Act[20/] ("ECPA") when interpreting the requirements of section 103(a). In addition, the FNPRM fails to give appropriate consideration to CALEA's legislative history. As a result, the FNPRM evaluates the various disputed capabilities in a statutory vacuum, misreading CALEA and broadening its requirements far beyond the limited scope that Congress intended.

"It is a fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme." *Davis v. Michigan Dept. of Treasury*, 489 U.S. 803, 809 (1989).[21/] CALEA fits precisely within

---

19/ 18 U.S.C. §§ 2510-22.

20/ *Id.* §§ 3121-27.

21/ *See also Fort Stewart Schools v. Federal Labor Relations Auth.*, 495 U.S. 641, 645 (1990) (stating that *Chevron* step one requires court to examine "the particular statutory language at issue, as well as the language and design of the statute as a whole"); *United States v. McGoff*, 831 F.2d 1071, 1080 (D.C. Cir. 1987) ("[I]t is well settled that, in interpreting a statute, the court will not look merely to a particular clause in which general words will be used, but will (continued...)

the statutory scheme Congress has established for electronic surveillance. Congress enacted Title III and the ECPA to authorize — and simultaneously set boundaries on — electronic surveillance by law enforcement, and Congress enacted CALEA to guarantee that law enforcement can effectively exercise its specified authority. CALEA's provisions must be interpreted in light of this overall statutory structure: Congress necessarily intended to require carriers to provide *only* those capabilities that law enforcement authorities may *lawfully* employ for electronic surveillance. Thus, Title III and the ECPA must be read as an implicit limitation on CALEA's requirements.

The FNPRM ignores this limitation. It states that "this proceeding does not involve any attempt to interpret statutes other than CALEA" and seeks only to identify the capabilities that law enforcement will need to access call content and call-identifying information.[22/] However, the capabilities needed by law enforcement are relevant only in the context of the information it lawfully may obtain.

CALEA's legislative history also makes clear that Congress did not intend CALEA to expand law enforcement's surveillance authority.[23/] FBI Director Freeh, for example, repeatedly emphasized in his spoken and prepared testimony to Congress that the FBI's proposed bill (which ultimately became CALEA) was meant only to "maintain technological capabilities commensurate with existing statutory authority — that is, to prevent advanced

---

21/ (...continued)
take in connection with it the whole statute . . . and the objects and policy of the law.") (quoting *Stafford v. Briggs*, 444 U.S. 527, 535 (1980)).

22/ FNPRM at ¶ 33.

23/ *See U S WEST Public Notice Comments* at 6-8.

telecommunications technology from repealing, de facto, *statutory* authority now existing and conferred to us by the Congress."[24/] And the House Judiciary Committee expressly recognized this principle, stating that the bill "will not expand" law enforcement's statutory authority to conduct electronic surveillance.[25/]

The legislative history similarly demonstrates that, in addition to seeking to leave law enforcement's *statutory authority* unchanged, Congress intended that the scope of information available to law enforcement would not be expanded. Director Freeh told Congress that CALEA "ensures a maintenance of the status quo . . . as it relates to the types of information obtainable through pen resister and trap and trace devices."[26/] And the House Judiciary Committee expressly relied on this testimony when it approved CALEA, highlighting Director Freeh's assurance that law enforcement would receive "no more and no less access to information than it had in the past."[27/] The Committee also said it "expects industry, law enforcement and the FCC to narrowly interpret" CALEA's assistance requirements.[28/] And even

---

24/ *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary on H.R. 4922 and S. 2375*, 103d Cong. 7 (1994) (emphasis added) (testimony of FBI Director Freeh) ("*March Hearing*"); *see also id.* at 6 (stating that the FBI "was not seeking any expansion of the authority Congress gave to law enforcement when the wiretapping law was enacted 25 years ago").

25/ H.R. Rep. No. 103-827, at 17, *reprinted in* 1994 U.S.C.C.A.N. at 3497.

26/ *March Hearing, supra*, at 32; *see also id.* at 40 ("Under the proposed legislation, law enforcement would acquire this dialing information *as it does today — no more no less.*").

27/ H.R. Rep. No. 103-827, at 22, *reprinted in* 1994 U.S.C.C.A.N. at 3502.

28/ *Id.* at 23, *reprinted in* 1994 U.S.C.C.A.N. at 3503.

DOJ/FBI has acknowledged that "Congress made clear that its intent in imposing assistance requirements on telecommunications common carriers was 'to preserve the status quo'."[29/]

In short, the overall statutory scheme that Congress enacted for electronic surveillance and CALEA's specific legislative history expressly demonstrate that CALEA's requirements are defined by the limits of Title III and the ECPA, as well as the reach of lawful electronic surveillance at the time CALEA was enacted. To be required under section 103(a), therefore, a capability must be consistent with Title III and the ECPA and not provide law enforcement with categories of information it has never before been able to obtain.

B. The Punch List and Location Information Capabilities Do Not Meet the Requirements of Section 103(a) or Section 107(b).

1. Content of subject-initiated conference calls

The FNPRM proposes to give law enforcement the capability to intercept the content of subject-initiated conference calls after the subject has dropped off.[30/] However, that capability goes beyond the scope of Title III. Moreover, in one of the few instances where the FNPRM considers CALEA's legislative history, it misreads and misinterprets the sole statement it cites.

The key to this issue lies in the difference between the capability made available under J-STD-025 and the *additional* capability included in the punch list. J-STD-025 already provides that law enforcement may intercept the contents of a subject-initiated conference call to

---

29/ Joint Petition for Expedited Rulemaking, filed by DOJ and FBI, Mar. 27, 1998, at 16 ("*DOJ/FBI Deficiency Petition*") (quoting H.R. Rep. No. 103-827, at 22, *reprinted in* 1994 U.S.C.C.A.N. at 3502).

30/ *See* FNPRM at ¶¶ 73-79.

the same extent that the intercept subject can hear the contents of that call.[31] What DOJ/FBI seeks is the additional, expanded ability to intercept other conversations of parties to the call, including those that the intercept subject *cannot* hear because he has, for example, dropped off the call.

In proposing this capability, the FNPRM relies on section 103(a)'s reference to communications carried to or from "equipment, facilities, or *services*" of a subscriber.[32] But Title III is narrower, requiring court orders to specify "the communications *facilities* as to which . . . authority to intercept is granted." 18 U.S.C. § 2518(4)(b) (emphasis added).[33] And a conference call does not involve the subject's "facilities" — the subscriber's CPE, loop, or port — after the subject leaves a call. Thus, the punch list requirement would exceed CALEA's lawful scope, as defined by Title III, by permitting law enforcement to continue monitoring a conference call after the call is no longer connected to the subject's facilities.

This capability also goes far beyond the "status quo" that DOJ/FBI originally said it sought to preserve. Conference calls existed long before the recent technological innovations

---

[31] *See* J-STD-025 § 4.5.1 ("The Circuit IAP (CIAP) shall access a multi-party circuit-mode communication (e.g., Three-Way Calling, Conference Calling, or Meet Me Conferences) *as it would be presented to the intercept subject.*") (emphasis added).

[32] *See* FNPRM at ¶ 77 (emphasis added) (citing 47 U.S.C. § 1002(a)(1)) .

[33] Title III does permit "roving" wiretaps that are not tied to specific facilities, *see* 18 U.S.C. § 2518(11)(b), but the statute exacts a *quid pro quo* — requiring court orders to identify the *specific person* whose conversations will be intercepted. Indeed, courts have upheld roving wiretaps as constitutional precisely because Title III requires such wiretaps to be person-specific. *See, e.g., United States v. Bianco*, 998 F.2d 1112, 1124 (2d Cir. 1993). The capability demanded by DOJ/FBI, however, would intercept communications from facilities that were never specified in a court order and of persons that were never identified as intercept subjects.

in telephony, and law enforcement agencies were not able to intercept conversations on a conference call when a subject was not on the call.[34/]

The FNPRM also relies on an excerpt from CALEA's legislative history as supposed evidence that this capability should be included in a Commission standard: a passage from the House report stating that one of CALEA's purposes "is to preserve the government's ability . . . to intercept communications involving . . . features and services such as call forwarding, speed dialing and conference calling."[35/] The FNPRM relies on this excerpt to *expand* law enforcement's powers and carriers' obligations, yet ignores the repeated theme of the legislative history that Congress expected the Act to be read narrowly to preserve the status quo.

In any event, the passage does not support the conclusion for which it is cited. In that passage, Congress said it sought to "preserve" the ability to intercept communications involving conference calls. As noted, DOJ/FBI's requested capability would *expand* law enforcement's ability to access those communications: For the first time, a person's private conversations would be subject to interception simply because he *previously* was on a conference call with an intercept subject.

Finally, even if this capability met the requirements of section 103(a), it would raise significant issues under section 107(b)(2), which requires that a Commission standard "protect the privacy and security of communications not authorized to be intercepted." *See* 47 U.S.C. § 1006(b)(2). By allowing law enforcement access to conversations not tied to an

---

34/ *See DOJ/FBI Deficiency Petition* at 30 (stating that the Interim Standard's conference call capability would "not amount to a reduction in the information that has been available to law enforcement under POTS").

35/ FNPRM at ¶ 77 (citing H.R. Rep. No. 103-827 at 9, *reprinted in* 1994 U.S.C.C.A.N. at 3489).

intercept subject's facilities and by subjecting *any* person's conversations to monitoring simply because at some point that person was on a conference call involving the subject, the capability would give law enforcement access to private conversations that Title III heretofore protected.

2. Party hold, join, drop on conference calls

As noted above, long before the adoption of CALEA, law enforcement was able to conduct electronic surveillance of conference calls. Throughout that time, parties had the capacity to drop conference call participants, put them on hold, and join new parties, and law enforcement was not able to obtain information about these changes.[36/] Nonetheless, and notwithstanding FBI Director Freeh's assurances to Congress that law enforcement would acquire call-identifying information under CALEA "*as it does today — no more no less*,"[37/] DOJ/FBI now demands access to party hold/join/drop information. The Commission should reject that demand. Including this capability would improperly expand law enforcement's existing surveillance ability.

The proposed capability also cannot be reconciled with CALEA's definition of call-identifying information.[38/] The FNPRM attempts to shoehorn party hold/join/drop messages into the definition by arguing that "party join information appears to identify the *origin* of a communication; party drop, the *termination* of a communication; and party hold, the temporary

---

36/ *DOJ/FBI Deficiency Petition* at 44 (admitting that law enforcement traditionally has not been able "to obtain information that a particular participant was placed on hold during, or dropped from, a multi-party call").

37/ *March Hearing, supra*, at 40.

38/ Section 102(2) of CALEA defines call-identifying information as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2).

origin, temporary *termination*, or re-*direction* of a communication."[39] But this interpretation ignores how Congress and the Commission have used the italicized words in other contexts.

"Termination" has always been used to refer to the final connection necessary to complete the circuit for a communication, not to refer to the end of a call. For example, a "terminating office" is the "switching center (*i.e.*, the central office) of the person you're calling."[40] The Commission's interpretation of "termination" in a myriad of other contexts makes this interpretation clear.[41] When interpreting the phrase "termination of telecommunications" in the context of section 251(b)(5), for example, the Commission understood Congress to mean "the switching of traffic . . . at the terminating carrier's end office switch (or equivalent facility) and delivery of that traffic from that switch to the called party's premises."[42] Thus, in J-STD-025, Subcommittee TR45.2 defined "termination" in the context of call-identifying information as "the number of the party ultimately receiving a call (e.g., answering party)."[43] CALEA's legislative history directly supports this interpretation,

---

39/ FNPRM at ¶ 85 (emphases added).

40/ *Newton's Telecom Dictionary* at 1033; *see also id.* at 1032 (defining "terminate" as "1. To connect a wire conductor to something, typically a piece of equipment. 2. To end one's telecommunications service or equipment rental").

41/ *See, e.g., International Telecharge, Inc., Complainant, v. Southwestern Bell Telephone Co. et al., Defendants*, File No. E-92-64 et al., Memorandum Opinion and Order, 11 FCC Rcd 10061, 10064, 10066, 10071-72 ¶¶ 4, 6, 27-29 (1996); *Teleconnect Company Complainant v. The Bell Telephone Company of Pennsylvania et al., Defendants*, File No. E-88-83 et al., Memorandum Opinion and Order, 10 FCC Rcd 1626, 1627-30 ¶¶ 4-6, 9, 13 (1995).

42/ *Implementation of the Local Competition Provisions in the Telecommunications Act of 1996*, CC Docket No. 96-98, First Report and Order, 11 FCC Rcd 15499, 16015 ¶ 1040 (1996).

43/ *See* J-STD-025, § 3 (defining "call-identifying information"). This definition of (continued...)

summarizing the statute's call-identifying information provisions as requiring carriers to "isolate expeditiously information identifying the *originating and destination numbers* of targeted communications."[44/]

The FNPRM likewise misinterprets the requirement that carriers provide law enforcement with the "origin" of any communication as call-identifying information. The FNPRM suggests that this requires carriers to send a message notifying law enforcement whenever a new communication begins or is restarted. Such an event would be described as the "origination" of a communication, not its "origin."[45/] The plain meaning of the "origin" of a communication is the "place" where the call begins; thus, as defined in J-STD-025, the origin of a call is "the number of the party initiating a call (e.g., calling party).[46/] J-STD-025 therefore

---

43/ (...continued)
"termination" does not make the word "destination" redundant in the statute's definition of call-identifying information. Based on its technical expertise, Subcommittee TR45.2 defined "destination" as "the number of the party to which a call is being made (e.g., called party)." With advanced features such as call forwarding, the destination and termination of a call will often be different, and both numbers will be needed by law enforcement.

44/ *See* H.R. Rep. 103-827, at 16, *reprinted in* 1994 U.S.C.C.A.N. at 3496 (emphasis added). Although the bill originally defined call-identifying information to include only the "origin and destination" of communications, the bill had already been amended to include "direction" and "termination" when the House Judiciary Committee made this statement about CALEA's requirements.

45/ *See, e.g., Oxford Dictionary and Thesaurus* 1051-52 (1996) (defining "originate" in temporal terms ("cause to begin; initiate") while defining "origin" in more physical and spatial terms ("a beginning or starting point; a derivation; a source (*a word of Latin origin*)").

46/ J-STD-025, § 3 (defining "call-identifying information").

provides the "origin" of each leg of a conference call, to the extent that information is available to the switch.[47]

3. Subject-initiated dialing and signaling information

The FNPRM tentatively concludes that subject-initiated dialing and signaling information that is reasonably available to carriers meets the assistance capability requirements of section 103(a)(2).[48] Although neither DOJ/FBI nor the FNPRM defines this capability with much detail, it apparently is meant to provide law enforcement with signals indicating a subject has used services such as call forwarding, call waiting, call hold, and three-way calling.[49] Thus, the capability would track a subject's manipulation of calls much in the same way as the party hold/join/drop capability discussed above in part II.B.2. And for many of the same reasons set forth there, the feature key and flash hook signals that DOJ/FBI is demanding under this capability do not meet CALEA's definition of "call-identifying information."

As discussed above, CALEA requires carriers to give law enforcement specific telephone numbers associated with a call, not the ability to track the course of every conversation and to know "to whom the subject is speaking at any point in the conversation."[50] J-STD-025 provides the information that CALEA requires. It permits law enforcement, for example, to find out whether and to what number a call has been forwarded. But once an intercept subject establishes a line of communications with another party, the "origin, direction, destination, and

---

47 *See* J-STD-025, § 5.4.5 (Origination message), § 5.4.10 (TerminationAttempt message).

48 *See* FNPRM ¶¶ 91-94.

49 *See id.*

50 *See DOJ/FBI Deficiency Petition* at 37.

termination" of that call are fixed. If the subject uses call-waiting or puts a party on hold, that action does not alter the "origin, direction, destination, and termination" of the original communication. Thus, the additional signaling demanded by DOJ/FBI is outside the scope of section 103(a).

4. Timing information

The FNPRM tentatively concludes that time stamp information meets the definition of call-identifying information under section 103(a)(2) of CALEA. It requests comment on what is a reasonable amount of time in which to require carriers to deliver the time-stamped messages to law enforcement.

This capability is a prime example of the "gold-plating" that Congress feared law enforcement would demand under CALEA.[51/] Under J-STD-025, carriers will provide call-identifying information in the vast majority of cases well within the timing requirements demanded by DOJ/FBI. In most cases, the relevant signaling information will be contained directly in the switch operating as the intercept access point, and the information will be conveyed to law enforcement nearly instantaneously. Indeed, DOJ/FBI admits that "the vast majority of carriers routinely and normally deliver call-identifying information as necessary to perform call setup and takedown in well under three seconds, commonly in a matter of microseconds."[52/]

51/ H.R. Rep 103-827, at 49, *reprinted in* 1994 U.S.C.C.A.N. at 3515.

52/ *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Reply Comments Regarding Standards for Assistance Capability Requirements, filed by DOJ and FBI, June 12, 1998, at 62 ("*DOJ/FBI Public Notice Reply Comments*").

However, DOJ/FBI demands that carriers be required to provide *all* call-identifying information within 3 seconds and with an accuracy of 100 milliseconds. That is not "reasonably available" to carriers within the meaning of section 103(a)(2). In a small percentage of cases, the necessary call-identifying information does not reside in the switch and would have to be accessed from elsewhere in the network. The time it takes to do this, plus any transmission delays resulting from occasional congestion in the network, would make DOJ/FBI's "3-second guarantee" difficult to achieve and thus an unreasonable demand.

Finally, when analyzing whether this capability is "cost-effective" under section 107(b), the Commission should bear in mind the very insignificant performance benefits that this capability would provide. Because this capability would provide access to additional information in only a small percentage of cases, it cannot justify the outlay of substantial funds.

5. Dialed digit extraction

The FNPRM tentatively concludes that post-cut-through digits are call-identifying information.[53/] In addition, the FNPRM requests comment on whether such information is reasonably available to carriers that originate calls.

Post-cut-through digits are not call-identifying information under section 103(a), at least for a local exchange carrier ("LEC") such as U S WEST. Digits that a subscriber dials after cut-through do not identify the "origin, direction, destination, or termination" of a call. From the LEC's perspective, the call is terminated at the interexchange carrier's platform, and the LEC has no special ability or reason to distinguish between these digits and other "content" of the call. Nor would the LEC have any way of deciphering whether the subscriber is using the

---

53/ *See* FNPRM ¶ 128.

digits to connect with another telephone number or, for example, to access an electronic bank account. Thus, such digits also are not "reasonably available" to the LEC.[54/]

Moreover, in evaluating this capability under section 107(b), the Commission should consider that law enforcement can obtain access to this information in at least two other ways: Obtain a pen register order for the intercept subject's interexchange carrier, or obtain a call content channel from a LEC and then decipher for itself the intercept subject's calling patterns. Therefore, costs associated with the requested capability are inherently unreasonable.

6. In-band and out-of-band signaling

The FNPRM asks for comment on the types of in-band and out-of-band signaling information that fall within section 103.[55/] In the first instance, it is up to DOJ/FBI to be more precise about what it wants and why, as well as to satisfy section 107(b). To date, DOJ/FBI has made only general demands for "signaling that identifies call progress,"[56/] and it has suggested various examples of signaling that might meet that definition.

The signaling discussed by the FNPRM — to indicate a subject has received a voice mail message — is not call-identifying information.[57/] Such signaling does not identify "the origin, direction, destination, or termination" of a communication to or from a subscriber; it

---

54/ Furthermore, CALEA's legislative history makes clear that the statute "is not intended to guarantee 'one-stop shopping' for law enforcement." H.R. Rep. No. 103-827, at 22, *reprinted in* 1994 U.S.C.C.A.N. at 3502. The House report also states that, if an advanced intelligent network directs a communication "to a different carrier, the subscriber's carrier only has the responsibility . . . to ensure that law enforcement can identify the new service provider handling the communication." *Id.*

55/ *See* FNPRM ¶ 99.

56/ *See DOJ/FBI Public Notice Reply Comments* at 55.

57/ *See* FNPRM ¶ 99.

informs a subject that someone has left a message for him or her. Indeed, the FNPRM does not even try to demonstrate how this signaling would fit within CALEA's definition of call-identifying information. Moreover, such a signal falls under CALEA's exemption for "information services," *see* 47 U.S.C. § 1002(b)(A), which CALEA expressly defines to include "a service that permits a customer to retrieve information from . . . information storage facilities." *Id.* § 1001(6)(B). A signal indicating that a voice mail message is waiting for retrieval would clearly be a part of such a service. CALEA's legislative history reinforces this conclusion. According to the House report, if a call to an intercept subject is redirected to a voice mail box, law enforcement may intercept that call just as it may intercept other calls to the subject that are redirected to another location.[58/] However, "the capability requirements only apply to those services or facilities that enable the subscriber to make, receive or direct calls."[59/] Signaling that indicates a subject has received a voice mail message is part of the voice mail service and does not allow a subscriber to "make, receive or direct calls."

7. Surveillance status/Continuity check tone

The FNPRM correctly concludes that section 103(a) does not require carriers to provide law enforcement with either surveillance status information or a continuity check tone.[60/] The requirement that carriers "shall ensure" that their facilities are capable of intercepting communications and isolating call-identifying information requires at most that carriers provide

---

58/ *See* H.R. Rep. No. 103-827, at 23, *reprinted in* 1994 U.S.C.C.A.N. at 3503; *see also id.* at 20, *reprinted in* 1994 U.S.C.C.A.N. at 3500 (noting that information service providers are not covered by CALEA but that "the call redirection portion of a voice mail service [is] covered by the bill").

59/ *See id.* at 23, *reprinted in* 1994 U.S.C.C.A.N. at 3503.

60/ *See* FNPRM ¶¶ 109, 114.

reliable electronic surveillance,[61] not that this "be proven or verified [by carriers] on a continual basis."[62]

Moreover, the Commission can be confident that carriers will, even in the absence of these capabilities, ensure that wiretaps remain operational.[63] U S WEST has a long history of providing highly efficient and reliable assistance to law enforcement, and it will continue to provide that same service after CALEA is fully implemented. U S WEST personnel promptly inform law enforcement if they detect any problems with wiretaps and pen registers. Such problems, in fact, have been extremely rare, and there is nothing in the record to suggest that they will become more common after CALEA's implementation. In the past three years, for example, U S WEST has implemented more than 3,000 wiretaps and pen registers on behalf of law enforcement. Once they were installed and operational, there were subsequent technical problems in no more than 2 percent of these surveillances.

If law enforcement officials suspect that a wiretap or pen register is not functioning correctly, U S WEST personnel are available 24 hours a day to verify its proper operation. Typically, law enforcement is the first to become aware of any problem with a wiretap, and they contact U S WEST's Court Order Processing Center ("COPC") for assistance with troubleshooting. In U S WEST's experience, even when problems have arisen at odd hours, law enforcement authorities generally have not availed themselves of U S WEST's 24-hour service and have simply waited until the next business day to work out the problems with COPC.

61/ *See U S WEST Public Notice Comments* at 23-24.

62/ FNPRM ¶ 109.

63/ *See id.* ¶ 110.

Thus, there is no basis for DOJ/FBI's suggestion that automated surveillance status information is urgently needed and that human assistance would be impractical to ensure that wiretaps and pen registers remain operational.

8. Feature status

The FNPRM correctly concludes that section 103 does not require carriers to implement the feature status information capability demanded by DOJ/FBI. As the Commission itself states, section 103(a) "does not require carriers to implement any specific quality control capabilities to assist law enforcement."[64] In any event, U S WEST has provided law enforcement with expeditious access to feature status information in the past and will do so in the future. The vast majority of wiretap orders require U S WEST's COPC to inform law enforcement of an intercept subject's features when the wiretap is installed. This information is available almost instantaneously through U S WEST's customer information databases and is provided to law enforcement when requested in a court order. In addition, if a court order requires that feature status information be available on a 24-hour basis, the intercept subject's feature status information is made accessible to law enforcement via U S WEST's Emergency Response Center, which handles 911 and other emergency services around the clock.

Moreover, law enforcement never before has had the unfettered access that DOJ/FBI now is demanding to carriers' databases, and DOJ/FBI's reasons for seeking this capability today are unconvincing. Intercept subjects, for example, were able to add second lines and custom calling features long before CALEA's enactment, and DOJ/FBI's assertion that the

---

[64] *See* FNPRM at ¶ 121.

"employees who could have serviced [manual] requests in the old environment do not exist today"[65] is simply incorrect.

9. Location information

Contrary to the FNPRM, the location information capability in J-STD-025 is not call-identifying information under section 103(a).[66] CALEA's definition of call-identifying information requires the provision of the "origin, direction, destination, [and] termination" of calls but not the "physical location" of the intercept subject. This omission is telling. As discussed above in part II.B.2, CALEA's definition of call-identifying information requires carriers to provide law enforcement with telephone numbers, not other characteristics of calls. Although law enforcement generally is able to derive a target's physical location from a telephone number for most wireline calls, that ability is incidental to the call-identifying information requirement and should not be read into the statute as an underlying mandate of CALEA.

DOJ/FBI's reliance on the language in section 103(a)(2) is misplaced. That section states that "*with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices* . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber." *See* 47 U.S.C. § 1002(a)(2) (emphasis added). DOJ/FBI and the FNPRM incorrectly infer from the italicized

---

[65] *See DOJ/FBI Public Notice Reply Comments* at 76.

[66] *See* FNPRM at ¶ 52. Although U S WEST voted in favor of J-STD-025 in the name of industry consensus, U S WEST had been a leader in opposing the inclusion of this capability in the industry standard. Indeed, even when U S WEST voted in favor of J-STD-025, it specifically noted on its ballot that it had reservations regarding the location information capability. Now that the Commission has opened this issue for comment, U S WEST again is reasserting its opposition to the inclusion of this capability in any Commission standard.

language that "call-identifying information" could include location information if acquired under some authority *other than* a pen register or trap-and-trace device order (*i.e.*, a Title III order).

This interpretation of CALEA does not make sense when placed in the context of the statutory regime governing electronic surveillance. Title III permits law enforcement to obtain the *contents* of communications, not their attributes.[67] Because location information is not content, the only means by which law enforcement might obtain location information would be through a pen register order.[68] But Congress specifically foreclosed that option in section 103(a)(2). Thus, Congress's language in section 103(a)(2) was intended to prevent law enforcement from getting location information under *any* circumstances.

CALEA's legislative history supports this view. It is true, as DOJ/FBI asserts, that CALEA's definition of call-identifying information once contained a broad exclusion of all location information. But DOJ/FBI is mistaken in its claim that this exclusion was simply moved to section 103(a)(2) and then narrowed to its present form.[69] Rather, the bill that the House Judiciary Committee reported to the House contained *both* the broad exclusion of location information in the definition of "call-identifying information" *and* the location language of

---

[67] *See* 18 U.S.C. § 2511(1) (defining "intercept" as "the aural or other acquisition of the *contents* of any wire, electronic, or oral communication") (emphasis added).

[68] Indeed, CALEA's language suggests that Congress thought call-identifying information was identical to (or a subset of) the information available under pen register orders. Whereas the ECPA authorizes law enforcement to obtain "the dialing and signaling information utilized in call processing," 18 U.S.C. § 3121(c), CALEA's definition of call-identifying information requires carriers to provide law enforcement with only the "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication," 47 U.S.C. § 1001(2).

[69] *See DOJ/FBI Public Notice Reply Comments* at 79.

section 103(a)(2).[20] In light of the House Report's categorical statement that the bill would not require carriers to provide "the physical location of targets,"[21] Congress apparently added the location language to section 103(a)(2) to re-emphasize the definitional exclusion. Congress's subsequent deletion of the definitional exclusion reflects a recognition that the location language of section 103(a)(2) achieved the same purpose.

III. THE COMMISSION SHOULD NOT IMPOSE NEW REGULATORY BURDENS ON PACKET-MODE COMMUNICATIONS AND SHOULD UNDER NO CIRCUMSTANCES REQUIRE CARRIERS TO SEPARATE HEADER INFORMATION FROM THE CONTENT OF SUCH COMMUNICATIONS.

The FNPRM opens a wide area of inquiry regarding packet-mode communications.[22] The Commission recognizes that the application of electronic surveillance requirements to packet-mode communications — the veritable backbone of the Internet — raises many new issues that will require both significant time and attention in order to resolve. U S WEST supports this prudent approach and urges the Commission not to impose any new regulations on emerging packet-mode technology in the absence of a full record concretely demonstrating both a clear need and the existence of technology that will minimize costs and other adverse effects.

If the Commission requires carriers to provide any call-identifying information on a packet-switched network, it should in no event obligate carriers to separate the "headers" from

---

[20] *See* H.R. Rep. No. 103-827, at 2-3.

[21] *Id.* at 16, *reprinted in* 1994 U.S.C.C.A.N. at 3496 (stating that the bill requires carriers to "[i]solate expeditiously information identifying the originating and destination numbers of targeted communications, but not the physical location of targets").

[22] *See* FNPRM ¶¶ 58-66.

content for provision to law enforcement. As TIA persuasively explained in its comments on the Public Notice, such a requirement is not technologically feasible.[73] Packet data is delivered in a layered stack structure, and carriers have neither the ability nor any business reason to monitor packet data streams and then decipher the various protocols in order to segregate headers from content. Indeed, placing such an obligation on carriers would hamper their efforts to speed the processing and routing of packet data. Even if carriers and manufacturers somehow developed a means of separating headers from content, the necessary analysis and processing of the packet stream would in all likelihood increase costs and diminish the performance of packet-switched services.

Moreover, the Commission should exclude from its standard *any* capability requirements applicable to packet-switched data services. Packet-mode technology is one of the leading forces in today's telecommunications revolution.[74] U S WEST has been a leader on this front, offering new services that provide high-speed access to the Internet.[75] Requiring carriers such as U S WEST to offer CALEA capabilities with respect to these packet-switched data services (*e.g.*, xDSL, frame relay, ATM) would inevitably impose heavy costs and slow their operation. Indeed, applying any surveillance requirements to such services would raise a host of

---

[73] *See Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Reply Comments of the Telecommunications Industry Association, filed June 12, 1998, at 12-17.

[74] *See generally Deployment of Wireline Services Offering Advanced Telecommunications Capability*, CC Docket No. 98-147, Memorandum Opinion and Order and Notice of Proposed Rulemaking, FCC 98-188, ¶¶ 6-8 (rel. Aug. 7, 1998) ("*Advanced Services NPRM*").

[75] *See* Petition of U S WEST Communications, Inc. for Relief from Barriers to Deployment of Advanced Telecommunications Services, filed Feb. 25, 1998, at 6-35.

technical challenges because of the fundamental differences between packet data transmission and conventional call processing. Such requirements would be particularly burdensome in the wireless context, where packet data technology — not to mention the technology needed for electronic surveillance — is truly in its infancy. In short, imposing CALEA requirements on packet-mode communications would frustrate the Commission's strongly expressed desire to encourage high-speed communications.[76] Such requirements also would run counter to section 107(b), which expressly directs the Commission to consider not only costs but also whether a capability "serve[s] the policy of the United States to encourage the provision of new technologies and services to the public." 47 U.S.C. § 1006(b)(4). To the extent CALEA obligations hamper the operation of new high-speed services, they will discourage their vigorous development and deployment.

The packet-mode requirements of J-STD-025 would have just such an effect. Because many packet-mode communications will avoid the circuit-switched network altogether, the J-STD-025 requirements for packet data therefore would require carriers and manufacturers to develop and install CALEA solutions for different network elements from those used in circuit-switched networks. Moreover, for a frame relay system, J-STD-025 requires carriers to peel off entire frames and deliver them through a Call Content Channel to law enforcement. In its discussions with industry, DOJ/FBI has requested that this information be delivered over a specified interface, which could limit the speed at which carriers can transmit the data to law enforcement. Unless the specified interface is of equivalent or higher speed than the surveillance service that sends the data, carriers will be forced to buffer the data in other network elements,

---

[76] *See Advanced Services NPRM at* ¶¶ 1-5.

such as routers. This either will either cause delays in the operation of those network elements or force carriers to expand their capacity. Thus, the requirements of J-STD-025 would hamper the performance of carriers' packet-switched networks or increase carriers' costs.

In short, the risks to advanced services and the Internet strongly suggest that the imposition of CALEA requirements on packet networks be deferred, at least until CALEA can be implemented without inhibiting the nation's nascent e-commerce industry.

IV. THE FNPRM CORRECTLY CONCLUDES THAT A COMMISSION STANDARD CAN BE IMPLEMENTED MOST EFFICIENTLY BY PERMITTING TIA'S SUBCOMMITTEE TR45.2 TO DEVELOP ANY NECESSARY TECHNICAL SPECIFICATIONS.

U S WEST supports the FNPRM's tentative conclusion that the Commission should remand any necessary technical standardization work to TIA's Subcommittee TR45.2.[77/] This would be the best way to ensure the efficient and reliable implementation of CALEA. Subcommittee TR45.2 already has been working on CALEA technical standards for nearly four years and, even during these Commission proceedings, has continued to cooperate with law enforcement to develop technical standards for the punch list capabilities. Allowing this work to continue would both hasten CALEA's implementation and ensure that the carriers are able to comply "by cost-effective methods." *See* 47 U.S.C. § 1006(b)(1). Moreover, the Commission clearly has authority to remand the technical work to Subcommittee TR45.2. Section 106 brings both manufacturers and carriers within the scope of CALEA's obligations, and section 107(b)(5) authorizes the Commission to "provide a reasonable time and conditions for compliance with and the transition to" any Commission standard. Thus, requiring Subcommittee TR45.2 to develop

---

77/ *See U S WEST Public Notice Comments* at 31-33.

any necessary technical standards would simply be a condition for the transition to a new Commission standard.[78/]

The Commission's expectation, however, that Subcommittee TR45.2 will be able to complete this process within 180 days after the release of the Report and Order in this proceeding probably is overly optimistic. The Commission is correct that Subcommittee TR45.2 has been working on CALEA's technical requirements for some time. But depending on how many of the punch list capabilities that the Commission ultimately adopts and on how the Commission defines those capabilities, developing a consensus on the necessary technical standards and having them subsequently approved by ballot (as required under American National Standards Institute ("ANSI") procedures) could take more than one year. The Commission should not underestimate the difficulty of defining technical standards, especially when the necessary capabilities will not be known at even a general level until the Commission completes this proceeding.

In an effort to speed this process, U S WEST has advocated that Subcommittee TR45.2 immediately take the procedural steps necessary before work can begin on any new standards. On December 8, 1998, the Enhanced Surveillance Services (ESS) working group within Subcommittee TR45.2 completed a proposal for a new project to revise J-STD-025 in response to any Commission order. The proposal seeks an accelerated development schedule, with work slated to start one month after a Commission order and to finish 14-17 months thereafter. This time frame is the minimum needed to develop and approve a technical standard

---

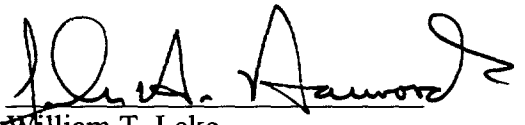
78/ *See also* 47 U.S.C. § 154(i) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this Act, as may be necessary in the execution of its functions.").

under ANSI and TIA procedures. Indeed, even DOJ/FBI seem to acknowledge that developing any new standards will take significantly longer than the 6 months proposed by the Commission: DOJ/FBI representatives were present at the December 8 ESS meeting, but they did not raise any objection to the 14-17 month time frame adopted there.

CONCLUSION

For the foregoing reasons, the Commission should reject the punch list capabilities demanded by DOJ/FBI, as well as the location information and packet-mode communications capabilities included within J-STD-025. If the Commission decides to revise the Interim Standard in any way, the Commission should remand any necessary technical standardization work to TIA's Subcommittee TR45.2.

Respectfully submitted,



William T. Lake
John H. Harwood II
Lynn R. Charytan
Todd Zubler
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420
(202) 663-6000

Kathryn Marie Krause
Edward M. Chavez
1020 19th Street, N.W.
Washington, DC 20036
(303) 672-2859

Counsel for

U S WEST, INC.

Of Counsel

Dan L. Poole
U S WEST, Inc.

December 14, 1998

CERTIFICATE OF SERVICE

I, Todd Zubler, hereby certify that, on this 14th day of December 1998, I have caused a copy of the foregoing "Comments of U S WEST, Inc." to be served either by hand or by first class U.S. mail, postage prepaid, on each of the parties set forth on the attached service list.

Todd Zubler

Todd Zubler

Honorable William E. Kennard
Federal Communications Commission
1919 M Street, N.W. - Room 814
Washington, D.C. 20554

The Honorable Harold Furchtgott-Roth
Federal Communicaitons Commission
1919 M Street, N.W. - Room 802
Washington, D. C. 20554

The Honorable Susan Ness
Federal Communications Commission
1919 M Street, N.W. - Room 832
Washington, D.C. 20554

The Honorable Michael Powell, Commissioner
Federal Communications Commission
1919 M Street, N.W. - Room 844
Washington, D.C. 20554

The Honorable Gloria Tristani
Federal Communications Commission
1919 M Street, N.W. - Room 826
Washington, D.C. 20554

David Wye
Telecommunications Policy Analyst
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W. - Room 5002
Washington, D.C. 20554

Lawrence Petak
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20554

Christopher J. Wright
General Counsel
Federal Communications Commission
1919 M Street, N.W. - Room 614
Washington, D.C. 20554

Daniel Phythyon, Chief
Wireless Telecommunications Bureau
Federal Communications Commissions
2025 M Street, N.W. - Room 5002
Washington, D.C. 20554

A. Richard Metzger, Chief
Common Carrier Bureau
Federal Communications Commission
1919 M Street, N.W. - Room 500B
Washington, D.C. 20554

Geraldine Matise
Chief, Network Services Division
Common Carrier Bureau
2000 M Street, N.W. - Room 235
Washington, D.C. 20554

Kent Nilsson
Deputy Division Chief
Network Services Division
Common Carrier Bureau
2000 M Streeet, N.W. - Room 235
Washington, D.C. 20554

David Ward
Network Services Division
Common Carrier Bureau
2000 M Street, N.W. - Room 210N
Washington, D.C. 20554

Charles Isman
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20554

Jim Burtle
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W. - Room 230
Washington, D.C. 20535

Marty Schwimmer, Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street, N.W., Room 290B
Washington, D.C. 20554

The Honorable Janet Reno
Attorney General
Department of Justice
Constitution Ave. & 10th Street, N.W.
Washington, D.C. 20530

The Honorable Stephen Colgate
Assistant Attorney General
Department of Justice
Constitution Ave. & 10th Street, N.W.
Washington, D.C. 20530

Stephen W. Preston, Assistant Attorney General
Douglas N. Letter, Appellate Litigation Counsel
Civil Division
Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530

The Honorable Louis J. Freeh
Director
Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Ave., N.W.
Washington, D.C. 20535

H. Michael Warren, Section Chief
CALEA Implementation Section
Federal Bureau of Investigation
14800 Conference Center Drive, Suite 300
Chantilly, VA 20151

David Sobel
Marc Rotenberg
Electronic Privacy Information Center
666 Pennsylvania Avenue, SE
Suite 301
Washington, D.C. 20003

Grant Seiffert, Director of Government Relations
Matthew J. Flanigan
Telecommunications Industry Association
1201 Pennsylvania Ave., N.W., Suite 315
Washington, D.C. 20004

Elaine Carpenter
Aliant Communications
1440 M Street
Lincoln, NE 68508

International Transcription Service, Inc.
1231 20th Street, N.W., First Floor
Washington, D.C. 20036

Pamela J. Riley/David A Gross
Airtouch Communications, Inc.
1818 N Street, N.W., Suite 320 South
Washington, D.C. 20036

Stewart A. Baker/Thomas M. Barba
J. Benjamin Ederington
Steptoe & Johnson LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036

Teresa Marrero
Teleport Communications Group, Inc.
Two Teleport Drive
Staten Island, NY 10311

Barry Steinhardt, President
Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco, CA 94103-4832

Michael Altschul, V.P. & General Counsel
Randall S. Coleman, V.P.
Cellular Telecommunications Industry Assoc.
1250 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20036

Gail L. Polivy
GTE Service Corporation
1850 M Street, N.W., Suite 1200
Washington, D.C. 20036

Carolyn G. Morris
US Department of Justice
Federal Bureau of Investigaitons
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Emilio W. Cividanes
Omnipoint Communications, Inc.
Piper & Marbury, LLP
1200 19th Street, N.W.
Washington, D.C. 20036

Andy Oram
O'Reilly & Assoc.
90 Sherman St.
Cambridge, MA 02140

Robert S. Foosaner/Lawrence R. Krevor
Laurel L. Holloway
Nextel Communications, Inc., Suite 425
1450 G Street, N.W.
Washington, D.C. 20005

L. Marie Guillory/Jill Canfield
National Telephone Cooperative Assoc.
2626 Pennsylvania Avenue, N.W.
Washington, D.C. 20037

David L. Nace/B. Lynn F. Ratnavale
Lukas, Nace, Gutierrez & Sachs Chartered
1111 19th Street, N.W., Suite 1200
Washington, D.C. 20036

Peter M. Connolly
Koteen & Naftalin
United States Cellular Corporation
1150 Connecticut Avenue, N.W.
Washington, D.C. 20036

Henry M. Rivera/Larry S. Solomon,
J. Thomas Nolan, M. Tamber Christian
Metricom, Inc.
Ginsburg, Feldman & Bress, Chtd.
1250 Connecticut Avenue, N.W.
Washington, D.C. 20036

Michael K. Kurtis/Jeanne W. Stockman
Kurtis & Associates, PC
2000 M Street, N.W., Suite 600
Washington, D.C. 20036

Mark C. Rosenblum/Ava B. Kleinman
Seth S. Gross
295 North Maple Avenue
Room 3252F3
Basking Ridge, NJ 07920

Kevin C. Gallagher, Sr. V.P &
General Counsel & Secretary
360° Communications Company
8725 West Higgins Road
Chicago, IL 60631

Steven Shapiro/A. Cassidy Sehgal
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004

Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco, CA 94103-4832

James R. RocheGlobecast
North America, Inc.
400 North Capitol Street, N.W.
Suite 880
Washington, D.C. 20001

Eric W. DeSilva
Stephen J. Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006

Caressa D. Bennet/Dorothy E. Cukier
Rural Telecommunications Group
Bennet & Bennet, PLLC
1019 19th Street, N.W., Suite 500
Washington, D.C. 20036

Stuart Polikoff, Sr. Regulatory &
Legislative Analyst
Lisa M. Zaina, V.P. & General Counsel
OPASTCO
21 Dupont Circle, N.W., Suite 700
Washington, D.C. 20036

Mark J. Golden, Sr. V.P., Industry Affairs
Robert Hoggarth
Personal Communications Industry Association
500 Montgomery Street, Suite 700
Alexandria, VA 22314-1561

Carol C. Harris/Christine M. Gill
Anne L. Fruehauf
Southern Communications Services
McDermott, Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005

M. Robert Sutherland
Theodore R. Kingsley
Bellsouth Corporation
1155 Peachtree Street, N.E., Suite 1700
Atlanta, GA 30309-3610

John T. Scott, III
Bell Atlantic Mobile, Inc.
Crowell & Moring, LLP
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Richard McKenna/John F. Raposa
GTE Service Corporation
600 Hidden Ridge, HQE03J36
P. O. Box 152092
Irving, TX 75015-2092

James D. Ellis/Robert M. Lynch
Durward D. Dupre, Lucille M. Mates,
Frank C. Magill
SBC Communications, Inc.
175 E. Houston, Room 4-H-40
San Antonio, TX 78205

Roy Neel/Mary McDermott/Linda Kent/
Keith Townsend/Lawrence E. Sarjeant
USTA
1401 H Street, N.W., Suite 600
Washington, D.C. 20005

William R. Roughton, Jr.
PrimeCo Personal Communications, L.P.
601 13th Street, Suite 320 South
Washington, D.C. 20005

Judith St. Ledger-Roty/Paul G. Madison
Paging Network, Inc.
Kelley, Drye & Warren, LLP
1200 19th Street, N.W., Suite 500
Washington, D.C. 20036

Michael P. Goggin
Bellsouth Cellular Corp.
1100 Peachtree Street, N.W., Suite 910
Atlanta, GA 30309-4599

Stephen L. Goodman
William F. Maher, Jr.
Halprin, Temple, Goodman & Sugrue
1100 New York Ave., N.W., Suite 650 East Tower
Washington, D.C. 20005

J. Lloyd Nault, II
BellSouth Telecommunications, Inc.
4300 BellSouth Center
675 West Peachtree Street, N. E.
Atlanta, GA 30375

Richard C. Barth/Mary E. Brooner
Motorola, Inc.
1350 I Street, N.W., Suite 400
Washington, D.C. 20005

Barbara J. Kern, Counsel
Ameritech Corporation
4H74
2000 Ameritech Center Drive
Hoffman Estates, Illinois 60196

Richard R. Metzger
Emily M. Williams
Association for Local
Telecommunications Services
888 17th Street, N.W., Suite 900
Washington, D.C. 20006

Kurt A. Wimmer, Esq.
Gerard J. Waldron, Esq.
Covington & Burling
1201 Pennsylvania Ave., N.W.
P. O. Box 7566
Washington, D.C. 20044-7566

Douglas I. Brandon
AT&T Wireless Services
1150 Connecticut Avenue, N.W.
Washington, D.C. 20036

Glenn S. Rabin
Federal Regulatory Counsel
Alltel Corporate Services, Inc.
655 15th Street, N.W., Suite 220
Washington, D.C. 20005

James X. Dempsey, Senior Staff Counsel
Daniel J. Weitzner, Deputy Director
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006

Martin L. Stern
Lisa A. Laventhal
Preston Gates Ellis & Rouvelas
Meeds LLP
1735 New York Avenue, N.W., Suite 500
Washington, D.C. 20006

Stephen G. Kraskin/Sylvia Lesse
Joshua Seidemann
Kraskin, Lesse & Cosson, LLP
2120 L Street, N.W., Suite 520
Washington, D.C. 20037

Joseph R. Assenzo, General Attorney
Sprint Spectrum, L.P.
4900 Main Street, 12th Floor
Kansas City, MO 64112

Charles M. Nalbone
BellSouth Personal Communications, Inc.
3353 Peachtree Road, N.E., Suite 400
Atlanta, GA 30326

Michael W. White
BellSouth Wireless Data, L.P.
10 Woodbridge Center Dr., 4th Floor
Woodbridge, NJ 07095-1106

Catherine Wang
ICG Telecom Group, Inc.
Swidler & Berlin, Chtd.
3000 K Street, N.W., Suite 300
Washington, D.C. 20007

Susan W. Smith, Director External Affairs
CenturyTel Wireless, Inc.
No. 4 Summer Place
3505 Summerhill Road
Texarkana, TX 75501

James F. Ireland/Theresa A. Zeterberg
Centennial Cellular Corp.
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W., Suite 200
Washington, D.C. 20006

Jill F. Dorsey, General Counsel/V.P.
Powertel, Inc.
1233 O.G. Skinner Drive
West Point, Georgia 31833

Gerald W. Fikis
Bell Emergis - Intelligent Signalling Technologies
78 O'Connor Street, Suite 410
Ottowa, Ontario, Canada KIP 3A4

James P. Lucier, Jr.
Director of Economic Research
Americans for Tax Reform
1320 18th Street, N.W., Suite 200
Washington, D.C. 20036

Lisa S. Dean, Director
Center for Technology Policy
Free Congress Foundation
717 Second Street, NE
Washington, D.C. 20002

Anita Seth, Director
Regulatory Policy Studies
Citizens for a Sound Economy
1250 H Street, N.W., Suite 700
Washington, D.C. 20005

Kenneth D. Patrick
Arch Communications Group, Inc.
Wilkinson, Barker, Knauer & Quinn, LP
2300 N Street, N.W.,
Washington, D.C. 20037

James W. McMahon, Superintendent
New York State Police
1220 Washington Avenue
Albany, New York 12226

Inv. Rodney Bradford
Ocean County Prosecutor's Office
P. O. Box 2191
Toms River, New Jersey 08754

Michael Carper, Assistant Gen. Counsel
Nextel Communications, Inc.
1505 Farm Credit Drive, Suite 100
McLean, VA 22102

Albert Gidari
Perkins Coie
1201 Third Ave., 40th Floor
Seattle, WA 98101

Johnnie L. Smith, Administrator
Division of Narcotics Enforcement
123 W. Washington Ave., 7th Floor
P. O. Box 7857
Madison, WI 53707-7857

Edward J. Wisniefski
Deputy Assistant Administrator
Office of Investigative Technology
Drug Enforcement Administration
8198 Terminal Road
Lorton, VA 22079

Det. Gene Marshall
OCB-Criminal Intelligence Section
Las Vegas Metropolitan Police
400 East Stewart Avenue
Las Vegas, Nevada 89101-2984